VISVESVARAYA TECHNOLOGICAL UNIVERSITY
"Jnana Sangama", Belagavi - 590 018

A project report on

"A SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION SYSTEM"

Submitted to Visvesvaraya Technological University, Belagavi
In partial fulfillment of the requirement for the degree of

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE & ENGINEERING

Submitted by

Bindhu K G	**(4BW13CS011)**
Chaithra C	**(4BW13CS012)**
Lakshmi Kavya P	**(4BW13CS026)**
Namratha D P	**(4BW13CS034)**

Under the guidance of:
Mr.ManuY M
Asst. Professor,
Computer Science and Engineering

HOD
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology,
B.G. Nagar - 571 448
Nagamangala Tq. Mandya Dist
Karnataka (India)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
BGS INSTITUTE OF TECHNOLOGY, B G NAGAR-571 448

2016-2017

BGS INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

B G Nagar – 571 448

CERTIFICATE

This is to Certify that the project work entitled **"A SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION SYSTEM" is** a bonafied work carried out by **Bindhu K G (4BW13CS011), Chaithra C (4BW13CS012), Lakshmi Kavya P (4BW13CS026), Namratha D P (4BW13CS034)** in partial fulfillment for the award of **Bachelor of Engineering** in **Computer Science & Engineering** of Visvesvaraya Technological University, Belagavi during the year 2016-17. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirements with respect to the project work prescribed by the University.

Signature of Guide	Signature of HOD	Signature of Principal
Mr. Manu Y M	**Prof.Shashikala S V**	**Dr.B K Narendra**
Asst. Prof., Dept. of CSE	**Head, Dept. of CSE**	**Principal**
BGSIT -BG Nagar	**BGSIT -BG Nagar**	**BGSIT -BG Nagar**
Manu.Y 22/6	Shashikala 22/6/17	Narendra

External Viva:

Name of the Examiners:	**Signature with Date:**
1. Shashikala SV	Shashikala 22/6/17
2. BHARATH MB	BHARATH MB 22/06/17

Shashikala
H O D
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology,
B.G. Nagara - 571 448.
Mandya Dist

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Bindhu K G

In recognition the publication of the manuscript entitled

Preventing A Shoulder Surfing Attack using Graphical Authentication System

published in Irjet Journal Volume 4 Issue 5 May 2017

HOD
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology
B.G. Nagar - 571 448
Nagamangala Tq. Mandya Dist
Karnataka (INDIA)

Impact Factor : 5.181

www.irjet.net

Editor in Chief
E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Chaithra C

In recognition the publication of the manuscript entitled

Preventing A Shoulder Surfing Attack using Graphical Authentication System

published in Irjet Journal Volume 4 Issue 5 May 2017

Editor in Chief

Impact Factor : 5.181

www.irjet.net

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Lakshmi Kavya P

In recognition the publication of the manuscript entitled

Preventing A Shoulder Surfing Attack using Graphical Authentication System

published in Irjet Journal Volume 4 Issue 5 May 2017

Editor in Chief

E-mail : editor@irjet.net

Impact Factor : 5.181

www.irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Namratha D P

In recognition the publication of the manuscript entitled

Preventing A Shoulder Surfing Attack using Graphical Authentication System

published in Irjet Journal Volume 4 Issue 5 May 2017

Shaikh

Editor in Chief

Impact Factor : 5.181

www.irjet.net

E-mail : editor@irjet.net

e-ISSN: 2395-0056 p-ISSN: 2395-0072

International Research Journal of Engineering and Technology (IRJET)

(An ISO 9001 : 2008 Certified Journal)

Is hereby awarding this certificate to

Manu Y M

In recognition the publication of the manuscript entitled

Preventing A Shoulder Surfing Attack using Graphical Authentication System

published in Irjet Journal Volume 4 Issue 5 May 2017

Shalini

Editor in Chief

Impact Factor : 5.181

www.irjet.net

E-mail : editor@irjet.net

ACKNOWLEDGEMENT

The completion of the project work involves the effort of many people. We are happy to have received a lot of help from all, during the course of this project work. And thus we take this opportunity to express my sincere thanks to all those who have guided, helped and encouraged us to emerge successfully.

We have immense pleasure in expressing our thanks to **Dr. B.K Narendra, Principal, BGSIT, BG Nagar** for having supported us in academic endeavors and for providing all the facilities for the successful completion of the project.

With respect we would like to thank our **HOD Prof.,Shashikala S.V, Prof,Head, Department of Computer Science and Engineering**, for her phenomenal support, keen interest which kept our spirit alive all through. We are thankful to our project co-ordinator **Mrs. Shwetha.K.R, Asst. Prof.** Department of Computer Science and Engineering, for her encouragement and help throughout the duration of the project.

We express our sincere concern to our project guide **Mr. Manu Y M, Asst.Prof, Department of Computer Science and Engineering**, for his patience and valuable advice and support that has been highly instrumental in the success of the project work.

We also would like to express our gratitude towards all our teaching and non-teaching staff for the kind co-operation during the course of work. Finally we would like to thank all our friends, parents who have been with us with their valuable suggestion.

Bindhu K G **(4BW13CS011)**
Chaithra C **(4BW13CS012)**
Lakshmi Kavya P **(4BW13CS026)**
Namratha D P **(4BW13CS034)**

H O D
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology
B.G. Nagar - 571 448
Nagamangala Tq. Mandya Dist
Karnataka (INDIA)

ABSTRACT

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short nor meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks.

With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

TABLE OF CONTENTS

LIST OF SNAPSHOTS

H O D
Dept. of Computer Science & Engg.
B.G.S. Institute of Technology,
B.G. Nagar - 571 448
Nagamangala Tq. Mandya Dist
Karnataka (INDIA)

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect . Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts . According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones.

Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically.However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs).

This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain. Therefore, an authentication scheme should be designed to overcome these vulnerabilities.

In this project, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time logininindicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

1.1 PROBLEM STATEMENT

Authentication based on passwords is used largely in applications for computer security and privacy.However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain.Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization.With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices.

This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks.Attackers can observe directly or use external recording devices to collect users' credentials.Objective of the project is to develop the application which resist Shoulder Surfing attacks in Graphical Authentication System.

- The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.
- The problem of how to increase password space than that of the traditional PIN.
- The problem of how to efficiently search exact password objects during the authentication phase.

- The problem of requiring users to memorize extra information or to perform extra computation during authentication.
- The problem of limited usability of authentication schemes that can be applied to some devices only.

1.2 GOALS AND OBJECTIVES

As the mobile marketing statistics compilation by Danyl, the mobile shipments had overtaken PC shipments in 2011, and the number of mobile users also overtaken desktop users at 2014, which closed to 2 billion . However, shoulder surfing attacks have posed a great threat to users' privacy and confidentiality as mobile devices are becoming indispensable in modern life. People may log into web services and apps in public to access their personal accounts with their smart phones, tablets or public devices, like bank ATM.

Shoulder-surfing attackers can observe how the passwords were entered with the help of reflecting glass windows, or let alone monitors hanging everywhere in public places.Passwords are exposed to risky environments, even if the passwords themselves are complex and secure. A secure authentication system should be able to defend against shoulder surfing attacks and should be applicable to all kinds of devices. Authentication schemes in the literature such as those in are resistant to shoulder-surfing, but they have either usability limitations or small password space. Some of them are not suitable to be applied in mobile devices and most of IEEE Transactions on Dependable and Secure Computing them can be easily compromised to shoulder surfing attacks if attackers use video capturing techniques like Google Glass.The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a period of time, and the authentication method being too complicated for users without proper education and practice.

In 2006, Wiedenbeck et al. proposed PassPoints in which the user picks up several points on an image during the password creation phase and re-enters each of these pre-selected click-points in a correct order within its tolerant square during the login phase. Comparing to traditional PIN and textual passwords, the Pass-Points scheme substantially increases the password space and enhances password memorability.

Unfortunately, this graphical authentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the PassPoints, we add the idea of using one-time session passwords and distracters to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.

1.3 SHOULDER SURFING ATTACKS

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public,they may expose their passwords to unknown parties unconsciously.People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window . Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets. Shoulder surfing attacks have gained more and more attention in the past decade. The following lists the research problems we would like to address in this study:

- The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.
- The problem of how to increase password space than that of the traditional PIN.
- The problem of how to efficiently search exact password objects during the authentication phase.
- The problem of requiring users to memorize extra information or to perform extra computation during authentication.
- The problem of limited usability of authentication schemes that can be applied to some devices only.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

In the past several decades, a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical based authentication systems. To keep this papeconcise, we will give a brief review of the most related schemes that were mentioned in the previous section. Many other schemes such as those in may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc.

In the early days, the graphical capability of handheld devices was weak; the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. We directly extract the figure from and show it in.If the drawing touche. the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology.

In 2005, Susan Wiedenbeck et al. introduced a graphical authentication scheme PassPoints , and at that time, handheld devices could already show high resolution color pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo.These features contain behavioral biometric characteristic. In other words, the attacker would have to imitate not only what the user draws, but also how the user draws it. However, these three authentication schemes are still all vulnerable to shoulder surfing attacks as they may reveal the graphical passwords directly to some unknown observers in public. Pixel squares selected by users as authentication passwords in PassPoints. (b) Authentication password drew by users and the raw bits recorded by the system database .

2.2 Graphical Password Authentication: Cloud Securing Scheme

S.Gurav(2014)

Graphical password is one of the alternative solution to alphanumeric password as it is very tedious process to remember alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use that application. One of the major reasons behind this method is according to psychological studies human mind can easily remember images than alphabets or digits. In this paper we are representing the authentication given to cloud by using graphical password. We have proposed cloud with graphical security by means of image password. We are providing one of the algorithms which are based on selection of username and images as a password. By this paper we are trying to give set of images on the basis of alphabet series position of characters in username. Finally cloud is provided with this graphical password authentication.

2.3"Why are pictures easier to recall than words?"Psychonomic Science

A. Paivio, T. Rogers, and P. Smythe (2000)

Pictures of objects were recalled significantly better than their names on the first two of four free recall trials. Recall for the two modes did not differ in intertriai organization but striking differences occurred as a function of input serial order. Picture superiority occurred for terminal input items on Trial 1, and both terminal and early items on Trial 2. The findings are discussed in terms of verbal and nonverbal (concrete) memory codes.

2.4."Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics.

T. Kwon, S. Shin, and S. Na(2014)

When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concern. To cope with this problem, previous methods presumed limited cognitive capabilities of a human adversary as a deterrent, but there was a pitfall with the assumption.

In this paper, we show that human adversaries, even without a recording device, can be more effective at eavesdropping than expected, in particular by employing cognitive strategies and by training themselves. Our novel approach called covert attentional shoulder surfing indeed can break the well known PIN entry method previously evaluated to be secure against shoulder surfing. Another contribution in this paper is the formal modeling approach by adapting the predictive human performance modeling tool for security analysis and improvement. We also devise a defense technique in the modeling paradigm to deteriorate severely the perceptual performance of the adversaries while preserving that of the user. To the best of our knowledge, this is the first work to model and defend the new form of attack through human performance modeling. Real attack experiments and user studies are also conducted.

2.5. S3PAS:A Scalable Shoulder-Surfing Resistant Textual-G.aphical Password Authentication Scheme.

I.Jermyn (2001)

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hiddencamera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shouldersurfing. In this paper, we propose a Scalable ShoulderSurfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-camera and spyware attacks. It can replace or coexist with conventional textual password systems without changing existing user password profiles. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS shows significant potential bridging the gap between conventional textual password and graphical password. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical anal,sis of the security level using S3PAS is also investigated.

2.6.FakePointer: An Authentication Scheme for Improving Security against Peeping Attacks Using Video Cameras.

T.Kwon(2014)

Peeping attacks in the real world are a threat to user authentication. What is worse, an emerging attack method such as video capture makes traditional measures against peeping attack insufficient. This paper presents a unique user authentication scheme named "fakePointer" as a solution to peeping attacks conducted by video capture. It makes it difficult for attackers to obtain a secret even if someone captures an authentication scene using a video camera. The fakePointer has two unique features to ensure security against such a peeping attack. One is that fakePointer provides a double-layered interface for a secret input. This interface makes it difficult for attackers to identify a legitimate user's secret even if they have a video record showing a target user's authentication action. The other feature is that fakePointer uses two secrets: a fixed secret and a disposable secret. This feature enables change of a secret input operation in each authentication, which is also a necessary feature for ensuring security. This feature makes it difficult to extract a secret by statistical inference even if an attacker has many video records of the same user.

CHAPTER 3

SYSTEM ANALYSIS

Introduction to System Analysis

A system is an orderly group of interdependent components linked together according to a plan to achieve a specific objective. Its main characteristics are organization, interaction, interdependence, integration and a central objective.

System Analysis

System analysis and design are the application of the system approach to problem solving generally using computers. To reconstruct a system the analyst must consider its elements output and inputs, processors, controls, feedback and environment.

Analysis

Analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. One aspect of analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related systems. During analysis data are collected on the available files decision points and transactions handled by the present system. This involves gathering information and using structured tools for analysis.

3.1 Existing System

In the Existing System Users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. Existing System is vulnerable to shoulder surfing attacks.

3.1.1 Disadvantages of the Existing System

- Existing System is vulnerable to shoulder surfing attacks.

  Type-I: Naked eyes.

  Type-II: Video captures the entire authentication process only once.

Type-III: Video captures the entire authentication process more than once.

3.2 Proposed System

To overcome

- The security weakness of the traditional PIN method
- The easiness of obtaining passwords by observers in public
- The compatibility issues to devices.

We introduced a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme.

3.2.1 Advantages of the Proposed System

- Proposed system is invulnerable to the all types Shoulder Surfing Attacks

  Such as,

  Type-I: Naked eyes.

  Type-II: Video captures the entire authentication process only once.

  Type-III: Video captures the entire authentication process more than once.
- It overcomes the security weakness of the traditional PIN method
- It overcomes the easiness of obtaining passwords by observers in public

3.3 FEASIBILITY STUDY

Feasibility is the determination of whether or not a project is worth doing. The process followed in making this determination is called feasibility Study. This type of study if a project can and should be taken.

In the conduct of the feasibility study, the analyst will usually consider seven distinct, but inter-related types of feasibility. Based on the different scnario and usage the unique feasibilities methods are implemented and observed.

Technical Feasibility: This is considered with specifying equipment and software that will successful satisfy the user requirement the technical needs of the system may vary considerably but might include:

- The facility to produce outputs in a given time.
- Response time under certain conditions.
- Ability to process a certain column of transaction at a particular speed.

Economic Feasibility: Economic analysis is the most frequently used technique for evaluating the effectiveness of a proposed system. More commonly known as cost / benefit analysis.
The procedure is to determine the benefits and savings are expected form a proposed system and a compare them with costs. It benefits outweigh costs; a decision is taken to design and implement the system will have to be made if it is to have a chance of being approved. There is an ongoing effort that improves in accuracy at each phase of the system life cycle.

Operational Feasibility: It is mainly related to human organization and political aspects. These points are considered are

- What changes will be brought with the system?
- What organizational structures are distributed?
- What new skills will be required?
- Do the existing system staff members have these skills?
- If not, can they be trained in the course of time?

3.4 ALGORITHMS

- Click Based Image Co-ordinate Generation
- Password String creation & Secret Code generation
- One Time Code (OTC) Generation
- OTC Verification
- Scroll Bar based Image Co-ordinate Generation
- Secret code Comparison

- MD5 (Message Digest 5) Algorithm.

3.5 System Requirements

3.5.1 Hardware Requirements

- System : Pentium IV 2.4 GHz.
- Hard Disk : 500 GB.
- Ram : 4 GB

3.5.2 Software Requirements

- Operating system : Windows XP / 7
- Coding Language : Java (Jdk 1.7)
- Web Technology : Servlet, JSP
- Web Server : TomCAT 7.0
- IDE : Eclipse Galileo
- Database : My-SQL 5.0
- UGI for DB : SQLyog
- JDBC Connection : Type 4 - Native Drive

3.6 Project Module Description

User Registration:

In this module user has to register by giving his information such as userid, user name, password ,valid e-mail id etc, and after giving this information, randomly three images will be assigned to the user, in those images he has to select the coordinate squares of the images as the graphical password. The details of coordinates of all images will be stored in the database with respect to the specific user.

Hash code generation:

After successful setting of the coordinates of the images ,those details will be stored in the database, concatenating all the three images coordinates and generate hash code for that and store in the database with respect to the user.

User Login Process:

Registered user will be login to the application by using his userid and password, if the userid and password is valid One Time Password(OTP) will be sent to the user's e-mail, whereas OTP contains the random pair of vertical and horizontal slider coordinate points of all the three images. After successful login , three assigned images will be displayed to the user with horizontal and vertical sliders , user has to set the horizontal and vertical sliders for all the three images ,where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating .if the hash code is matched with the existing hash code user can successful enter in to the home page , else, process ends and login page will display.

Admin:

Admin has to login to his account by the authenticated user name and password. Admin can able to view all the users details, who are successfully registered.

CHAPTER 4

SYSTEM DESIGN

4.1 Logical Design

Design for WebApps encompasses technical and non-technical activities. The look and feel of content is developed as part of graphic design; the aesthetic layout of the user interface is created as part of interface design; and the technical structure of the WebApp is modeled as part of architectural and navigational design.

This argues that a Web engineer must design an interface so that it answers three primary questions for the end-user:

- Where am I? – The interface should (1) provide an indication of the WebApp has been accessed and (2) inform the user of her location in the content.
- What can I do now? – The interface should always help the user understand his current options- what functions are available, what links are live, what content is relevant.
- Where have I been; where am I going? – The interface must facilitate navigation. Hence it must provide a "map" of where the user has been and what paths may be taken to move elsewhere in the WebApp.

4.2 Design goals

The following are the design goals that are applicable to virtually every WebApp regardless of application domain, size, or complexity.

1. Simplicity
2. Consistency
3. Identity
4. Visual appeal
5. Compatibility.

Design leads to a model that contains the appropriate mix of aesthetics, content, and technology. The mix will vary depending upon the nature of the WebApp, and as a consequence the design activities that are emphasized will also vary.

The activities of the Design process:

1. Interface design-describes the structure and organization of the user interface. Includes a representation of screen layout, a definition of the modes of interaction, and a description of navigation mechanisms. Interface Control mechanisms- to implement navigation options, the designer selects form one of a number of interaction mechanism;
   Interface Design work flow- the work flow begins with the identification of user, task, and environmental requirements. Once user tasks have been identified, user scenarios are created and analyzed to define a set of interface objects and actions.
2. Aesthetic design-also called graphic design, describes the "look and feel" of the WebApp. Includes color schemes, geometric layout. Text size, font and placement, the use of graphics, and related aesthetic decisions.
3. Content design-defines the layout, structure, and outline for all content that is presented as part of the WebApp. Establishes the relationships between content objects.
4. Navigation design-represents the navigational flow between contents objects and for all WebApp functions.
5. Architecture design-identifies the overall hypermedia structure for the WebApp. Architecture design is tied to the goals establish for a WebApp, the content to be presented, the users who will visit, and the navigation philosophy that has been established.
   a. Content architecture, focuses on the manner in which content objects and structured for presentation and navigation.
   b. WebApp architecture, addresses the manner in which the application is structure to manage user interaction, handle internal processing tasks, effect navigation, and present content. WebApp architecture is defined within the context of the development environment in which the application is to be implemented.

6. Component design-develops the detailed processing logic required to implement functional components.

4.3 Database Design

MySql is a relational database management system, which organizes data in the form of tables. MySQL is one of many databases servers based on RDBMS model.

This model manages the seer of data that attends three specific things-data structures, data integrity and data manipulation.

m_admin

Fields

Field	Type	Null	Key	Extra
Id	int(11)	NO	PRI	
Adminid	varchar(50)	YES		
Adminname	varchar(50)	YES		
Adminpass	varchar(50)	YES		
Gender	varchar(50)	YES		
Email	varchar(100)	YES		
Phone	varchar(20)	YES		
City	varchar(100)	YES		

Table 1: Admin details.

The details of the admin are stored in the format as shown in Table 1. The details such as mentioned in the above as taken as input.

m_user

Fields

Field	Type	Null	Key	Extra
u_no	int(10)	NO	PRI	auto_increment
u_id	varchar(100)	YES		
u_txtpwd	varchar(100)	YES		
u_name	varchar(50)	YES	MUL	
u_gender	varchar(10)	YES		
u_email	varchar(100)	YES		

u_phone	varchar(20)	YES		
u_city	varchar(50)	YES		
random_image1	varchar(100)	YES		
random_image2	varchar(100)	YES		
random_image3	varchar(100)	YES		
selectedlocation1	varchar(100)	YES		
selectedlocation2	varchar(100)	YES		
selectedlocation3	varchar(100)	YES		
hash_key	varchar(50)	YES		

Table 2: User details.

With MySQL cooperative server technology we can realize the benefits of open, relational systems for all the applications. MySQL makes efficient use of all systems resources, on all hardware architecture; to deliver unmatched performance, price performance and scaleability.

m_user_otp

Fields

Field	Type	Null	Key	Extra
Id	int(11)	NO	PRI	auto_increment
Uid	varchar(50)	YES		
image1	varchar(50)	YES		
image2	varchar(50)	YES		
image3	varchar(50)	YES		
randomrow1	int(11)	YES		
randomcol1	int(11)	YES		
randomrow2	int(11)	YES		
randomcol2	int(11)	YES		
randomrow3	int(11)	YES		
randomcol3	int(11)	YES		
horizantal_image	int(11)	YES		
vertical_image	int(11)	YES		
m_locations	varchar(50)	YES		

hash_key	varchar(50)	YES		

Table 3: User Otp details.

The user OTP will be sent to the mail and are stored at the datatbase in the following format as shown in the Table 3. The information is extracted whenever required by the admin.

CHAPTER 5

SYSTEM IMPLEMENTATION

5.1 System Architecture

Systems implementation is the process of:

1. defining how the information system should be built (i.e., physical system design),
2. ensuring that the information system is operational and used,
3. ensuring that the information system meets quality standard (i.e., quality assurance).

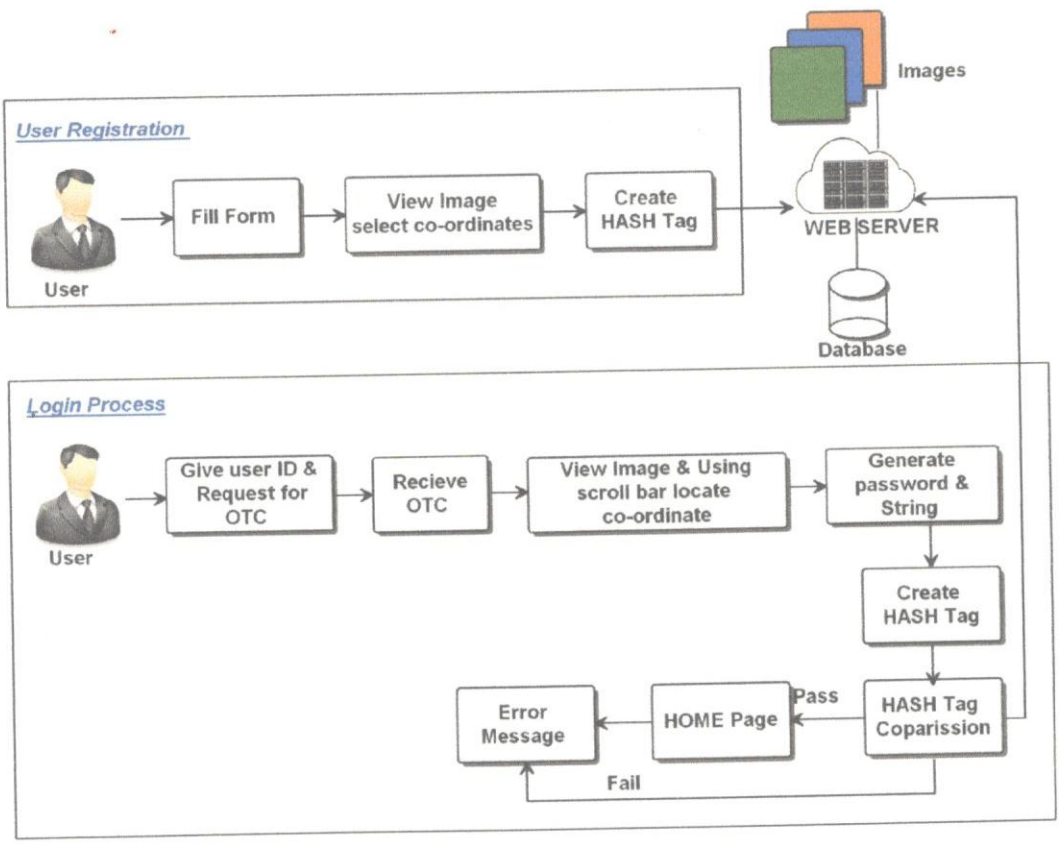


Fig 5.1.1: System Architecture.

The Fig 5.1.1 shows the system architecture of this project, in which the web server acts as the connecting medium between the back-end and the front-end operations in the project.

The user module has 3 main tasks such as filling the form, viewing the image and selecting the co-ordinates and creating the hash tags.

The login module has various modules giving the user id , requesting the OTP , receiving the OTC , viewing the image , using the scroll bars and locating the co-ordinates. Next generation of password and stirng , creating the hash tag , next the hash tag co-parission , next the going the home page, else if any interruots occur the returing back to home page is done.

On one end there are images stored for setting passwords . On the other end , the database is stored and accessed through various backend software such as mysql etc.,

5.2 Use case diagrams

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved.

5.2.1 Admin:

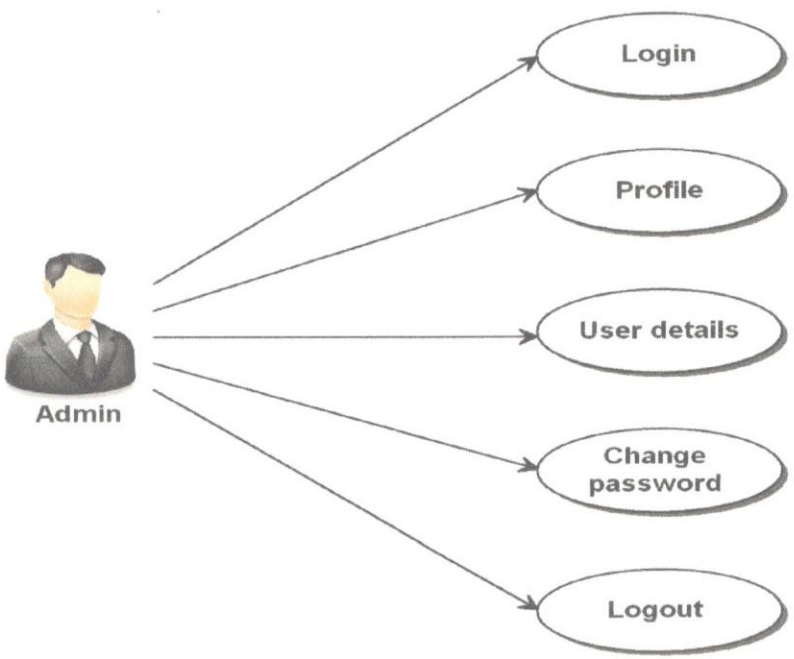


Fig 5.2.1: Use case diagram for Admin.

This diagram can identify the different types of users of a system and the different use cases and often be accompanied by other types of diagrams as well.

5.2.2 User:

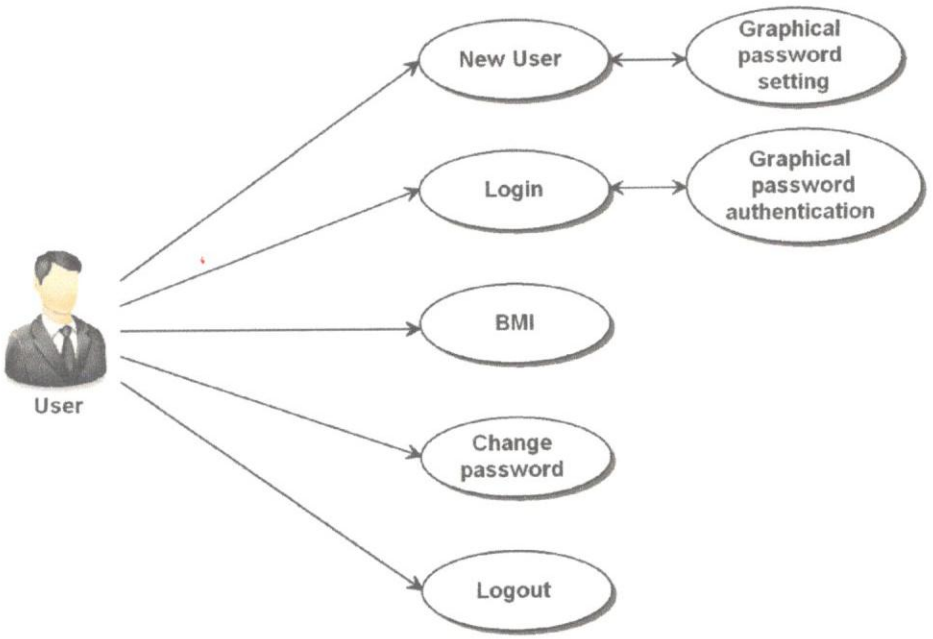


Fig 5.2.2: Usecase diagram for User.

These are various process which occurs during the login process of user.Here the user has many modules such as new user, login, BMI, change password, logout. New user also has a process graphical password setting which is interactive. Also login has an interactive process as graphical process authentication.

5.3 Sequence Diagram:

A sequence diagram is an interaction diagram that shows how objects operate with one another and in what order . It's a construct of a message sequence chart.

A sequence diagram shows, as parallel vertical lines(life lines),different processes or objects that live simultaneously and as horizontal arrows that messages exchanged between them in order in which they occur.

Sequence diagrams are sometimes known as event diagram or event scenario.

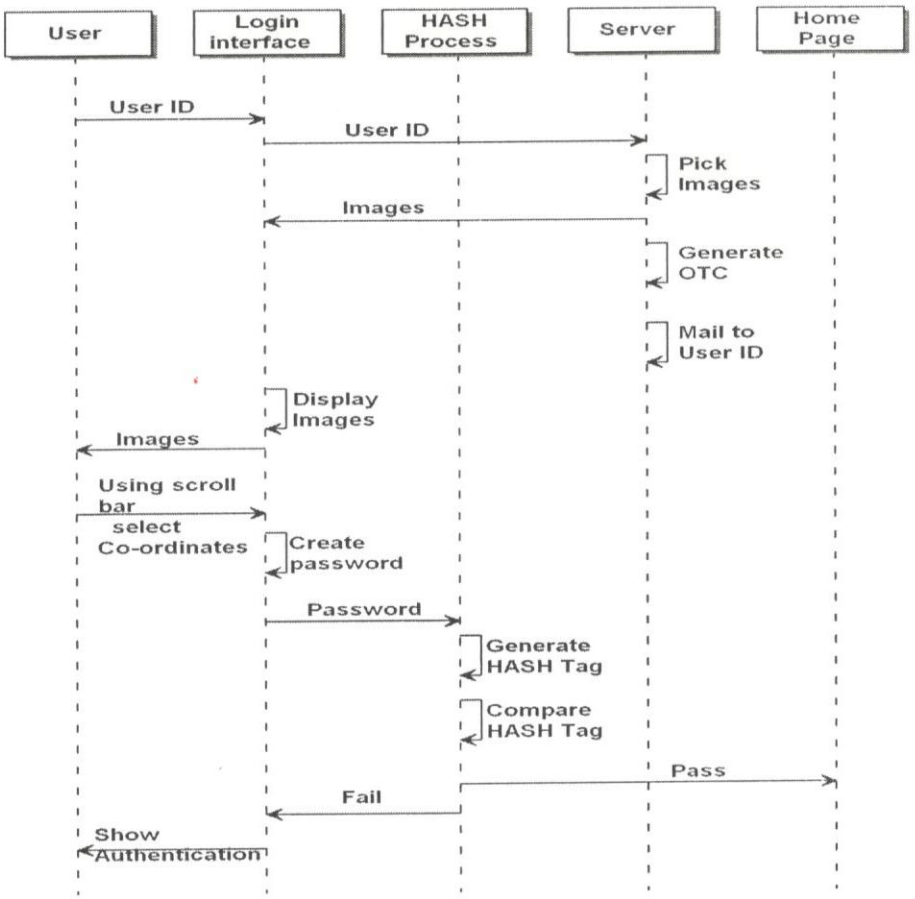


Fig 5.3.1: Sequence Diagram.

The above Figure 5.3.1 refers the sequence diagram of the process.There are five process as user, login interface, hash process, server and home page.

5.4 Context Analysis Diagram

The context diagram shows the system under consideration as a single high-level process and then shows the relationship that the system has with other external entities .

A system context diagram (SCD) in engineering is a diagram that defines the boundary between the system, or part of a system, and its environment, showing the entities that interact with it. This diagram is a high level view of a system. It is similar to a block diagram.

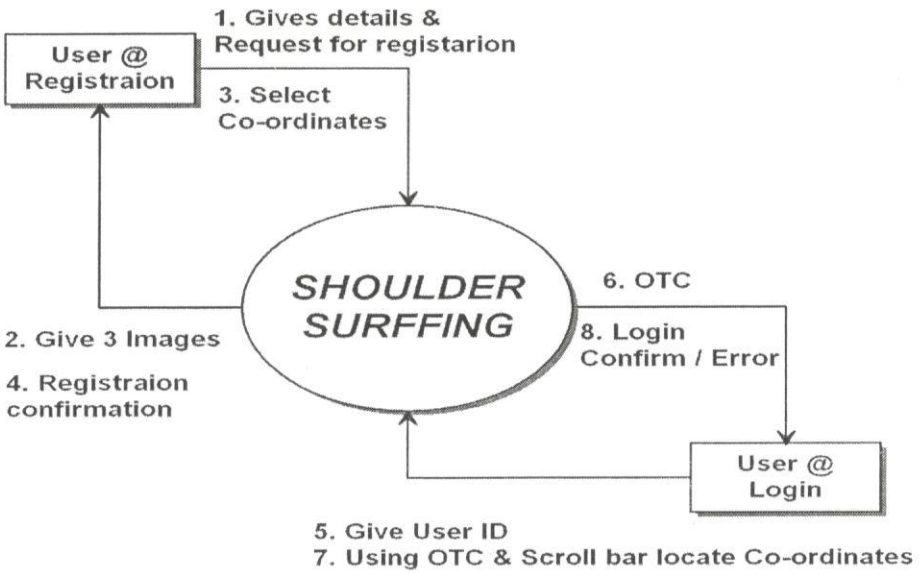


Fig 5.4.1: Context Analysis Diagram.

Another name for this diagram is a context level data-flow diagram or a level-0 data flow diagram. The process goes on as shown the Fig 5.4.1.

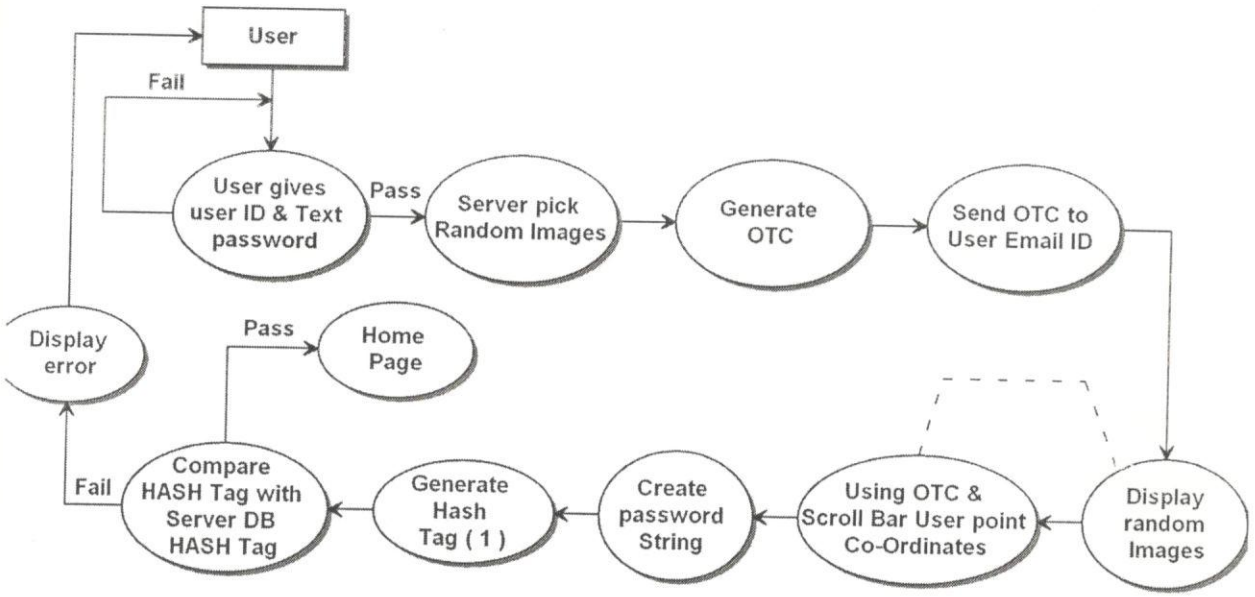


Fig 5.4.2: Data Flow Diagram for user.

Once after the user logs in the process runs as shown in the above data flow figure 5.4.2 based on the responses given by the user in each step .

CHAPTER 6

TESTING

Definition

Unit testing is a development procedure where programmers create tests as they develop software. The tests are simple short tests that test functionally of a particular unit or module of their code, such as a class or function.

Using open source libraries like cunit, oppunit and nun it (for C, C++ and C#) these tests can be automatically run and any problems found quickly. As the tests are developed in parallel with the source unit test demonstrates its correctness.

6.1 Validation and System Testing

Validation testing is a concern which overlaps with integration testing. Ensuring that the application fulfils its specification is a major criterion for the construction of an integration test. Validation testing also overlaps to a large extent with System Testing, where the application is tested with respect to its typical working environment. Consequently for many processes no clear division between validation and system testing can be made. Specific tests which can be performed in either or both stages include the following.

- **Regression Testing:** Where this version of the software is tested with the automated test harness used with previous versions to ensure that the required features of the previous version are skill working in the new version.

- **Recovery Testing:** Where the software is deliberately interrupted in a number of ways off, to ensure that the appropriate techniques for restoring any lost data will function.

- **Security Testing:** Where unauthorized attempts to operate the software, or parts of it, attempted it might also include attempts to obtain access the data, or harm the software installation or even the system software. As with all types of security determined will able to obtain unauthorized access and the best that can be achieved is to make .

- **Stress Testing:** Where abnormal demands are made upon the software by increasing the rate at which it is asked to accept, or the rate t which it is asked to produce information. More complex tests may attempt to crate very large data sets or cause the software to make excessive demands on the operating system.

- **Performance testing:** Where the performance requirements, if any, are checked. These may include the size of the software when installed, type amount of main memory and/or secondary storage it requires and the demands made of the operating when running with normal limits or the response time.

- **Usability Testing:** The process of usability measurement was introduced in the previous chapter. Even if usability prototypes have been tested whilst the application was constructed, a validation test of the finished product will always be required.

- **Alpha and beta testing:** This is where the software is released to the actual end users. An initial release, the alpha release, might be made to selected users who be expected to report bugs and other detailed observations back to the production team. Once the application changes necessitated by the alpha phase can be made to larger more representative set users, before the final release is made to all users.

The final process should be a Software audit where the complete software project is checked to ensure that it meets production management requirements. This ensures that all required documentation has been produced, is in the correct format and is of acceptable quality. The purpose of this review is: firstly to assure the quality of the production process and by implication construction phase commences. A formal hand over from the development team at the end of the audit will mark the transition between the two phases.

- **Integration Testing**:Integration Testing can proceed in a number of different ways, which can be broadly characterized as top down or bottom up. In top down integration testing the high level control routines are tested first, possibly with the middle level control structures present only as stubs.

Subprogram stubs were presented in section2 as incomplete subprograms whic'. are only present to allow the higher. Level control routines to be tested.

Top down testing can proceed in a **depth-first** or a **breadth-first** manner. For depth-first integration each module is tested in increasing detail, replacing more and more levels of detail with actual code rather than stubs. Alternatively breadth-first would processed by refining all the modules at the same level of control throughout the application .in practice a combination of the two techniques would be used. At the initial stages all the modules might be only partly functional, possibly being implemented only to deal with non-erroneous data. These would be tested in breadth-first manner, but over a period of time each would be replaced with successive refinements which were closer to the full functionality. This allows depth-first testing of a module to be performed simultaneously with breadth-first testing of all the modules.

The other major category of integration testing is **Bottom Up Integration Testing** where an individual module is tested form a test harness. Once a set of individual module have been tested they are then combined into a collection of modules ,known as builds, which are then tested by a second test harness. This process can continue until the build consists of the entire application. In practice a combination of top down and bottom-up testing would be used. In a large software project being developed by a number of sub-teams, or a smaller project where different modules were built by individuals. The sub teams or individuals would conduct bottom-up testing of the modules which they were constructing before releasing them to an integration team which would assemble them together for top-down testing.

6.2 Unit Testing:

Unit testing deals with testing a unit as a whole. This would test the interactior of many functions but confine the test within one unit. The exact scope of a unit is left to interpretation. Supporting test code, sometimes called Scaffolding, may be necessary to support an individual.

This type of testing is driven by the architecture and implementation teams. This focus is also called black-box testing because only the details of the interface are visible to the test. Limits that are global to a unit are tested here.

In the construction industry, scaffolding is a temporary, easy to assemble and disassemble, frame placed around a building to facilitate the construction of the building. The construction workers first build the scaffolding and then the building. Later the scaffolding is removed, exposing the completed building. Similarly, in software testing, one particular test may need some supporting software. This software establishes can a correct evaluation of the test take place. The scaffolding software may establish state and values for data structures as well as providing dummy external functions for the test. Different scaffolding software may be needed form one test to another test. Scaffolding software rarely is considered part of the system.

Sometimes the scaffolding software becomes larger than the system software being tested. Usually the scaffolding software is not of the same quality as the system software and frequently is quite fragile. A small change in test may lead to much larger changes in the scaffolding.

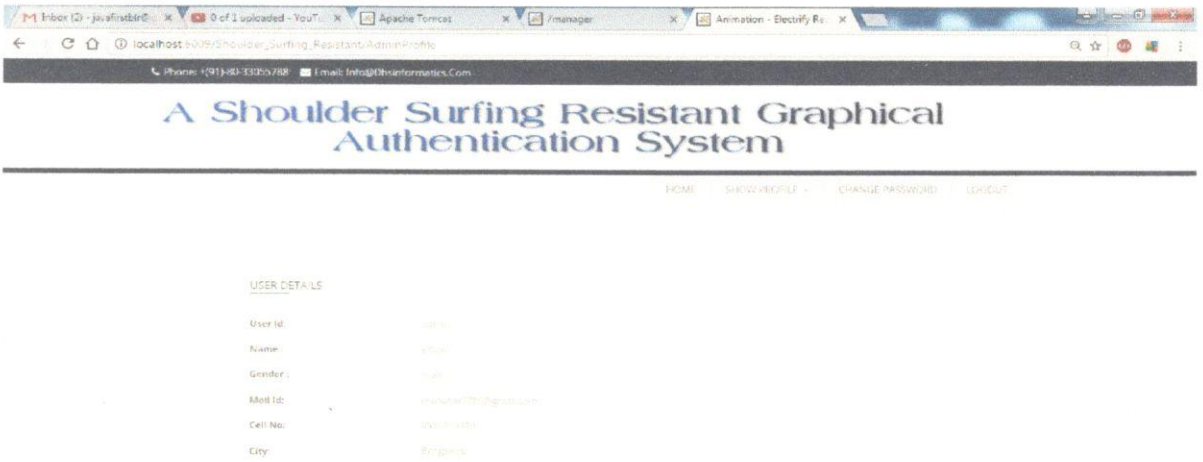
Internal and unit testing can be automated with the help of coverage tools. Analyzes the source code and generated a test that will execute every alternative thread of execution. Typically, the coverage tool is used in a slightly different way. First the coverage tool is used to augment the source by placing information prints after each line of code. Then the testing suite is executed generating an audit trail. This audit trail is analyzed and reports the percent of the total system code executed during the test suite. If the coverage is high and the untested source lines are of low impact to the system's overall quality, then no more additional tests are required.

CHAPTER 7

RESULTS AND SNAPSHOTS

7.1 Login Page

7.1.1 Admin home page



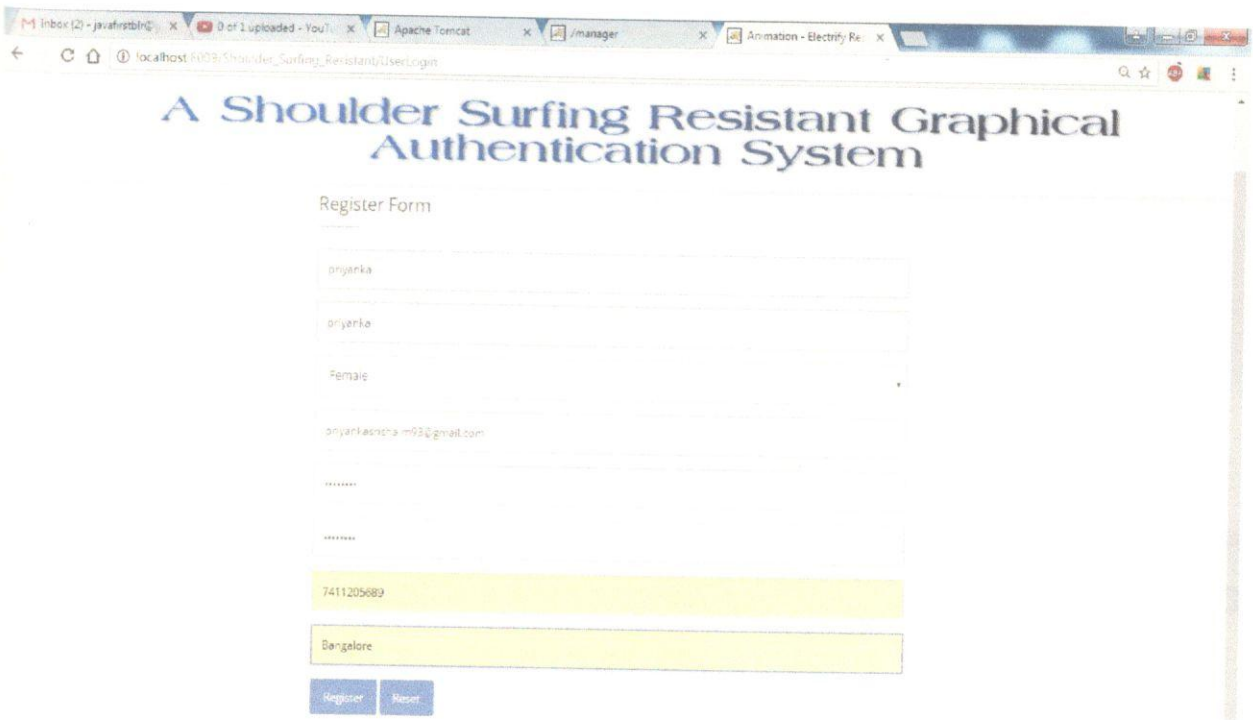
Snapshot 7.1.1: Admin home page.

The home page is the first page that appears when this application is opened , this page contains various blocks for which data should be input by the user. The details like userid , name of the user , gender , mail-id , cell number and city are take as input from the user for sending the OTP during the registration time. Snapshot 7.1 is the page which appears after the user login is done.

7.1.2 New User Registration

This page saves or register the user details of the user. It asks for various details like name , username , gender , email-id , password , mobile number and location of the user. This page is used for the new user registration.

Snapshot 7.1.2 acts as a registration form for any new user who require authentication for their content. After the Register button is pressed the future process continues else if the Reset button is chosen the details are again vanished or deleted for new data.

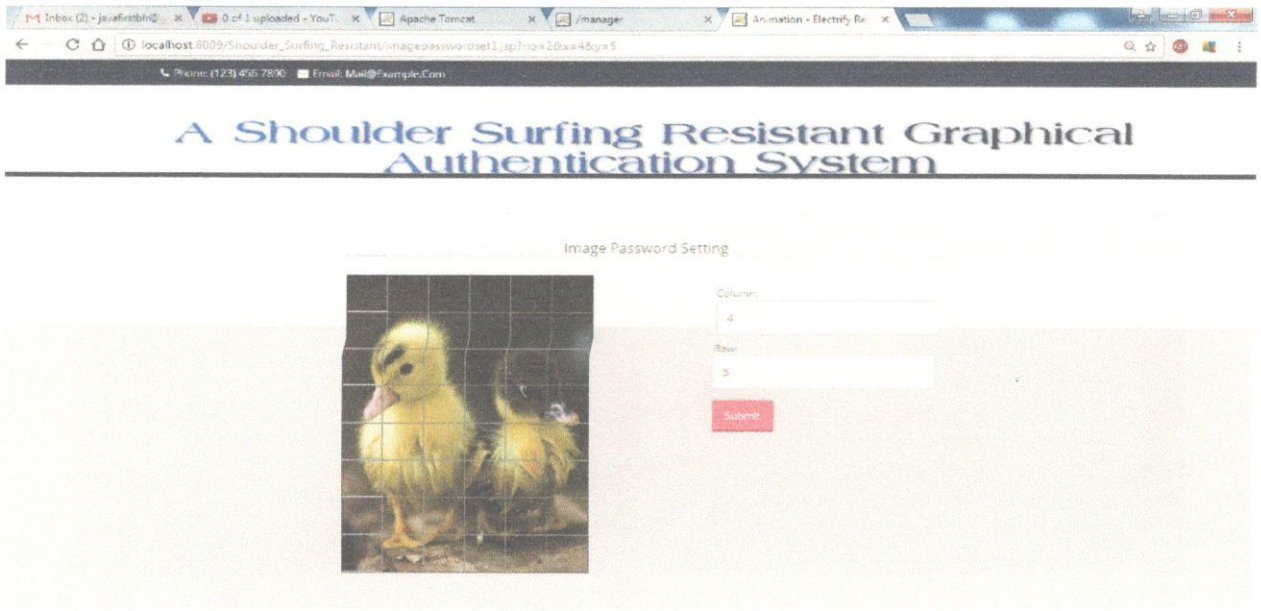


Snapshot 7.1.2: New User Registration.

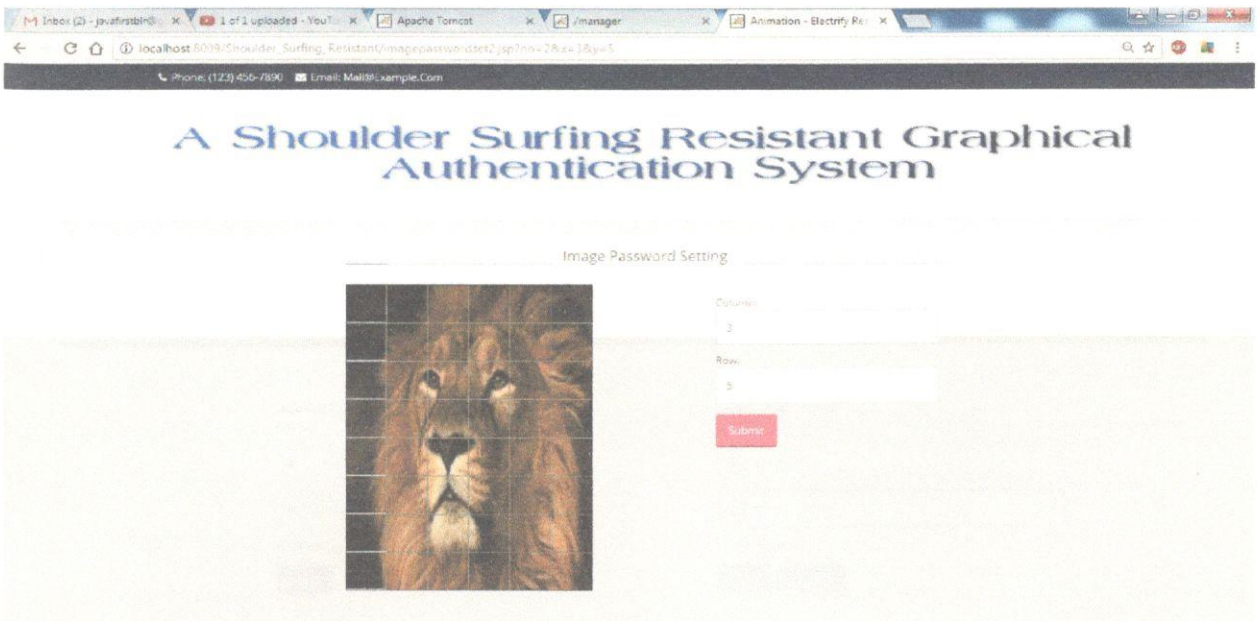
7.2 Image password settings

This involves 3 images for choosing the password which are divided into rows and columns . The number of images is set by the admin , not mandatory that it must be 3.After the registration process,the page will be generated by giving the rows and coloumn as shown above.After giving the rows and coloumn.Enter the submit button.

Here coloumn 4 and row 5 are given in the image. For the first authentication of this process the password is set as shown in Snapshot 7.3. These images are divided into rows and columns and upon the user choosing the part of the image the OTP is generated to the registered mail-id or to the respective contact number of the user.

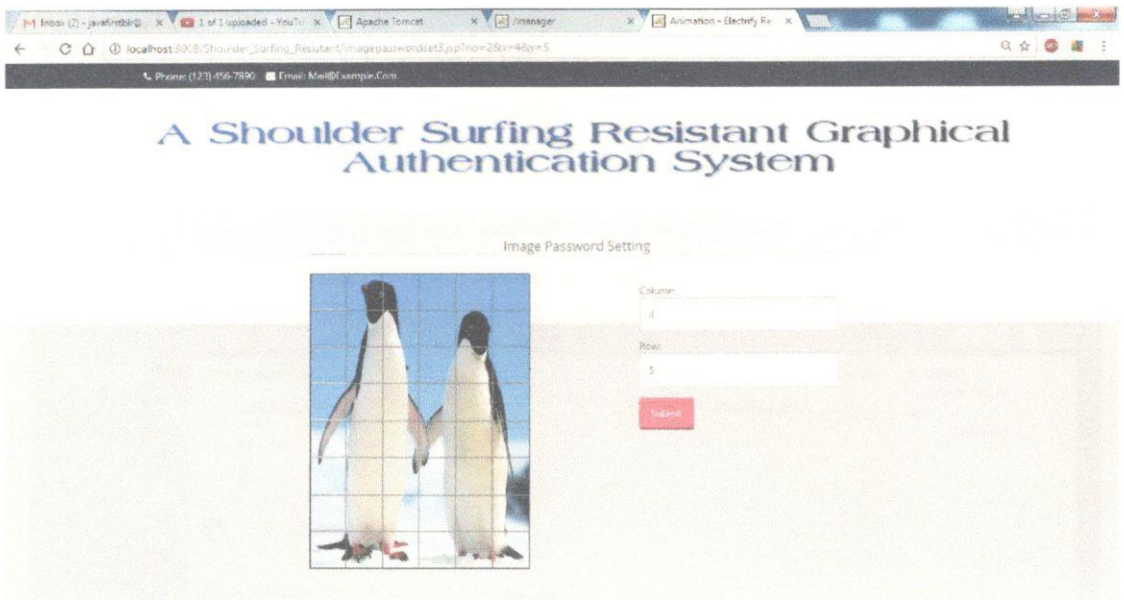


Snapshot 7.2.1: Image1.



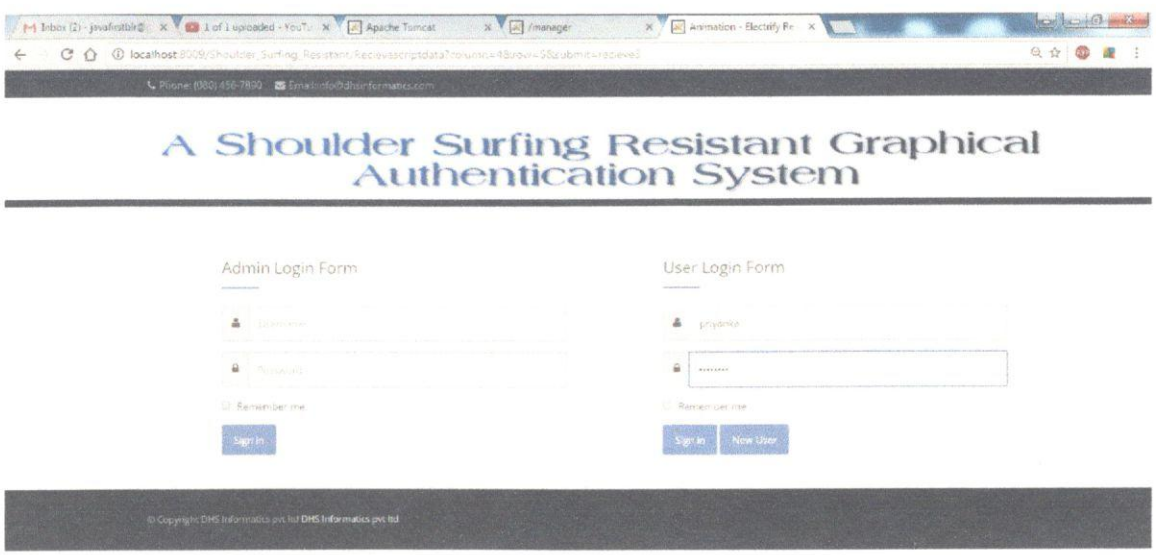
Snapshot 7.2.2: Image 2.

Same process for the image password setting will be followed for the upcoming images also. Again the coloumn 3 and rows 5 are entered and enter the submit button,again the third image will be generated.



Snapshot 7.2.3: Image3.

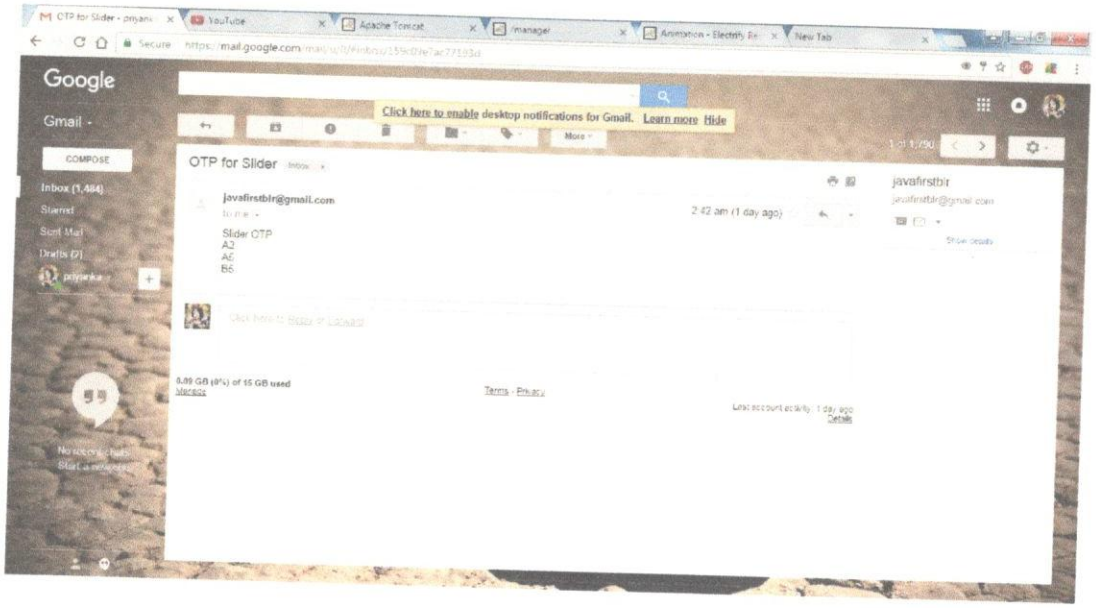
The screenshots of images in 7.2.1,7.2.2 and 7.2.3 are those which are divided into rows and columns . These images are set by the user for selecting the co-ordinates . The number of images should also be set by the admin.



Snapshot 7.2.4: User Login

After the image passward setting the user login process will be generated.The user needs to login to the form.

The user name and the password given during the time of the registration should be input to this page. The authentication is provided after the login of this page as shown in Snapshot 7.6 is done.

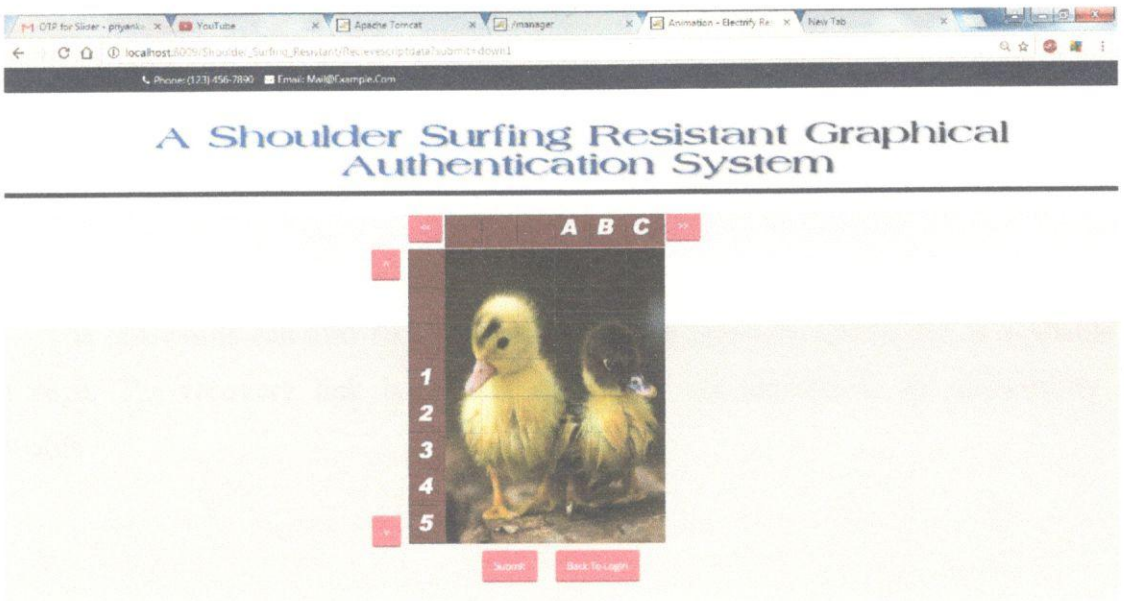


Snapshot 7.2.5: OTP from mail.

After the login process the OTP message will be sent to the mail. The OTP will be received by the user as shown in the Snapshot 7.7. Here for every login process new OTP will be generated so there is less chance of hacking. Using the received OTP's the image authentication is done by choosing the respective co-ordinates.

The scroll bars are provided here using which are co-ordinates are matched . The images which appear during the selection of the part of the image are totally different to those images that appear while matching the co-ordinates according to the received OTP that are obtained through mail-id or through the cell phones.

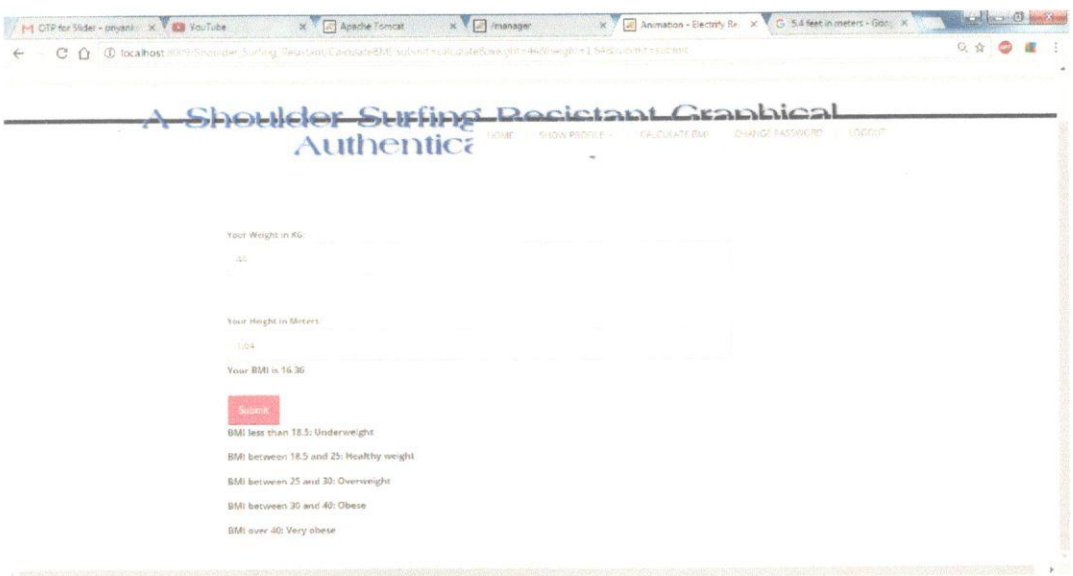
Since email is considered as confidential amongst all other medium of communication, we better choose the medium to be mail because if phone lines are damaged or line connections are not established properly.



Snapshot 7.2.6: Rearranging the co-ordinates.

After receiving the OPT from mail, now we are going to match the passaword what we had given before by mentioning the rows and coloumn and with the new passaword generated by the OPT to the mail. By scrolling and matching the passwards the web page will get opened.

The Snapshot 7.8 shows the use of the scroll bars using which the password is set. The images are divided based on the quality of the image quality.



Snapshot 7.2.7: Calculate BMI.

After the page is opened, we can see above screenshot we created a small application regarding to calculate BMI that is body mass index.If we entered the weight of the body it will give approximate height value to us.

For example as shown in the screenshot. The Snapshot 7.9 shows the application that is existed after the login is done. This application is just to give an example of how the existence of the operations once the login is done.

The passwords can also be recovered using the recovery option that is available in the main page. The recovery link is sent in scnario of the inexistence or inavailabity of the passwords .

CONCLUSION AND FUTURE ENHANCEMENT

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones.

To overcome this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009.Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4. "Realuser," http://www.realuser.com/.

[5] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies,
vol. 63, no. 1-2, pp. 102–127, 2005.

[8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

[10] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords?
a field trial investigation," PEOPLE AND COMPUTERS, pp. 405–424, 2000.

A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron,and M. Fischer, "Vip: a approach to user authentication," in Proceedings of the Working Conference on Advanced Interfaces.ACM, 2002, pp. 316–323.

B. Ives, K. Walsh, and H. Schneider, "The domino effect of passwordreuse," unications of the ACM, vol. 47, no. 4, pp. 75–78,2004.

Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering, ster Diving, and Shoulder Surfing. Elsevier Science,

T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are powerful than expected," IEEE Transactions on Systems, Man, and Cybernetics: Systems, 4, no. 6,pp. 716–727, June 2014.

"Google glass snoopers can steal your passcode with a glance," www.wired.com/2014/06/google-glass-snoopers-cansteal- your-passcode-with-a-glance/.

M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakestlinka human/computer ction approach to usable and effective security," BT technology journal, vol. 19, no. 3, pp. 31,2001.

"Mobile marketing statistics compilation,"http://www.smartinsights.com/mobile-eting/mobilemarketing-tics/mobile-marketing-statistics/.

D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to are," in Proceedings of International conference on security and management, 2004.

D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure ord entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-n Interaction

al Interest Group (CHISIG) of Australia. Canberra, Australia:

Press. Citeseer, 2005.

M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using -based password entry," in Proceedings of the 3rd symposium on Usable privacy and ity. ACM,

pp. 13–19.

APPENDIX

vaScript

aScript is a script-based programming language that was developed by Netscape mmunication Corporation. JavaScript was originally called Live Script and renamed as aScript to indicate its relationship with Java. JavaScript supports the development of both nt and server components of Web-based applications. On the client side, it can be used to e programs that are executed by a Web browser within the context of a Web page. On the er side, it can be used to write Web server programs that can process information submitted a Web browser and then update the browser's display accordingly

Even though JavaScript supports both client and server Web programming, we prefer aScript at Client side programming since most of the browsers supports it. JavaScript is ost as easy to learn as HTML, and JavaScript statements can be included in HTML uments by enclosing the statements between a pair of scripting tags

<Script> ..... </Script>

<Script Language = "JavaScript">

JavaScript statements

</Script>

re are a few things we can do with JavaScript

- Validate the contents of a form and make calculations.
- Add scrolling or changing messages to the Browser's status line.
- Animate images or rotate images that change when we move the mouse over them.
- Detect the browser in use and display different content for different browsers.
- Detect installed plug-ins and notify the user if a plug-in is required.
- We can do much more with JavaScript, including creating entire application.

JavaScript and Java are entirely different languages. A few of the most glaring differences are:

- Java applets are generally displayed in a box within the web document; JavaScript can affect any part of the Web document itself.
- While JavaScript is best suited to simple applications and adding interactive features to Web pages; Java can be used for incredibly complex applications.

There are many other differences but the important thing to remember is that JavaScript and Java are separate languages. They are both useful for different things; in fact they can be used together to combine their advantages.

- JavaScript can be used for Sever-side and Client-side scripting.
- It is more flexible than VBScript.
- JavaScript is the default scripting languages at Client-side since all the browsers supports it.

Java Technology

Initially the language was called as "oak" but it was renamed as "Java" in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architecture neutral) language that could be used to create software to be embedded in various consumer electronic devices.

- Java is a programmer's language.
- Java is cohesive and consistent.
- Except for those constraints imposed by the Internet environment, Java gives the programmer, full control.
- Finally, Java is to Internet programming where C was to system programming.

Importance of Java To The Internet

Java has had a profound effect on the Internet. This is because; Java expands the Universe of objects that can move about freely in Cyberspace. In a network, two categories of objects are transmitted between the Server and the Personal computer. They are: Passive information and Dynamic active programs.

The Dynamic, Self-executing programs cause serious problems in the areas of Security and probability. But, Java addresses those concerns and by doing so, has opened the door to an exciting new form of program called the Applet.

Java Can Be Used To Create Two Types Of Programs

Applications and Applets: An application is a program that runs on our Computer under the operating system of that computer. It is more or less like one creating using C or C++. Java's ability to create Applets makes it important. An Applet is an application designed to be transmitted over the Internet and executed by a Java –compatible web browser. An applet is actually a tiny Java program, dynamically downloaded across the network, just like an image. But the difference is, it is an intelligent program, not just a media file. It can react to the user input and dynamically change.

Features of Java Security

Every time you that you download a "normal" program you are risking a viral infection. Prior to java, most users did not download executable programs frequently, and those who did scan them for viruses prior to execution. Most users still worried about the possibility of infecting their systems with a virus. In addition, another type of malicious program exists that must be guarded against. This type of program can gather private information, such as credit card numbers, bank account balances, and passwords. Java answers both these concerns by providing a "firewall" between a network application and your computer.

When you use a java-compatible web browser, you can safely download java applets without fear of virus infection or malicious intent.

Portability

For programs to be dynamically downloaded to all the various types of platforms connected to the internet, some means of generating portable executable code is needed .as you will see, the same mechanism that helps ensure security also helps create portability. Indeed, java's solution to these two problems is both elegant and efficient.

The Byte Code

The key that allows the Java to solve the security and portability problems is that the output of Java compiler is Byte code. Byte code is a highly optimized set of instructions designed to be executed by the Java run-time system, which is called the Java Virtual Machine (JVM). That is, in its standard form, the JVM is an interpreter for byte code.

Translating a Java program into byte code helps makes it much easier to run a program in a wide variety of environments. The reason is, once the run-time package exists for a given system, any Java program can run on it.

Although Java was designed for interpretation, there is technically nothing about Java that prevents on-the-fly compilation of byte code into native code. Sun has just completed its Just

In Time (JIT) compiler for byte code. When the JIT compiler is a part of JVM, it compiles byte code into executable code in real time, on a piece – by –piece, demand basis. It is not possible to compile an entire Java program into executable code all at once, because Java performs various run-time checks that can be done only at run time. The JIT compiles code, as it is needed, during execution

Java Virtual Machine (JVM)

Beyond the language, there is the Java virtual machine. The Java virtual machine is an important element of the Java technology. The virtual machine can be embedded within a web browser or an operating system. Once a piece of Java code is loaded onto a machine, it is verified. As part of the loading process, a class loader is invoked and does byte code verification makes sure that the code that's has been generated by the compiler will not corrupt the machine that it's loaded on. Byte code verification takes place at the end of the compilation process to make sure that is all accurate and correct. So byte code verification is integral to the compiling and executing of Java code.

Java programming uses to produce byte codes and executes them. The first box indicates that the Java source code is located in a. Java file that is processed with a Java compiler called javac. The Java compiler produces a file called a. class file, which contains the byte code.

Overall Description

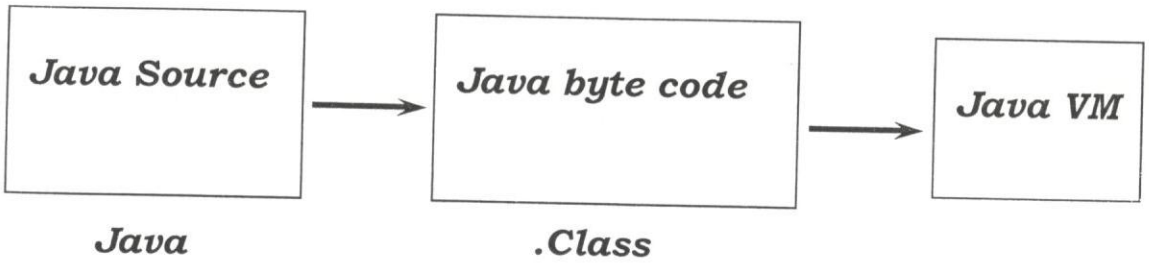


Fig : Picture showing the development process of JAVA Program.

The Class file is then loaded across the network or loaded locally on your machine into the execution environment is the Java virtual machine, which interprets and executes the byte code.

Java Architecture

Java architecture provides a portable, robust, high performing environment for development. Java provides portability by compiling the byte codes for the Java Virtual Machine, which is then interpreted on each platform by the run-time environment. Java is a dynamic system, able to load code when needed from a machine in the same room or across the planet.

Compilation of code

When you compile the code, the Java compiler creates machine code (called byte code) for a hypothetical machine called Java Virtual Machine (JVM). The code is written and compiled for one machine and interpreted on all machines. This machine is called Java Virtual Machine.

Sample Coding

AdminLogin.java

```
package com.admin;

import java.awt.image.BufferedImage;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Map;
import java.util.Random;

import javax.imageio.ImageIO;
import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;

import com.DAOFactory.Admin;
import com.DAOFactory.User;
import com.util.Send_SMS_Service;

public class AdminLogin extends HttpServlet
{
   RequestDispatcher rd = null;

   @Override
   protected void doPost(HttpServletRequest req, HttpServletResponse resp)        throws
ServletException, IOException
   {

      try
      {
            String submit=req.getParameter("submit");

            if(submit.equals("signin"))
            {
                  HttpSession hs=req.getSession();

                  String uid=req.getParameter("name").trim();
                  String pass=req.getParameter("pass").trim();
```

```
                    boolean flag=Admin.checkAdmin(uid,pass);

                    if(flag)
                    {

                            hs.setAttribute("adminid",uid);

                            rd = req.getRequestDispatcher("/jsp/Admin/adminhome.jsp");
                            rd.forward(req, resp);
                    }
                    else
                    {
                             RequestDispatcher
rd=req.getRequestDispatcher("index.jsp?no=2");
                            rd.forward(req, resp);
                    }
            }


        }
catch (Exception e)
        {
                System.out.println("********* Exception In New User Servlet ********\n");
                e.printStackTrace();
        }

    }

}
```